(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
3 mars 2005 (03.03.2005)

PCT

(10) Numéro de publication internationale
WO 2005/020538 A2

(51) Classification internationale des brevets[7] : H04L 29/06

(21) Numéro de la demande internationale :
PCT/FR2004/001849

(22) Date de dépôt international : 13 juillet 2004 (13.07.2004)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
03/09086 24 juillet 2003 (24.07.2003) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6 Place d'Alleray, F-75015 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **TRANSY, Estelle** [FR/FR]; 23, rue Victor Hugo, F-92130 Issy les Moulineaux (FR). **DELMOND, Fréderic** [FR/FR]; 80, rue de la Roquette, F-75011 Paris (FR). **NGUYEN NGOC, Sébastien** [FR/FR]; 16, rue Fillassier, F-92140 Clamart (FR).

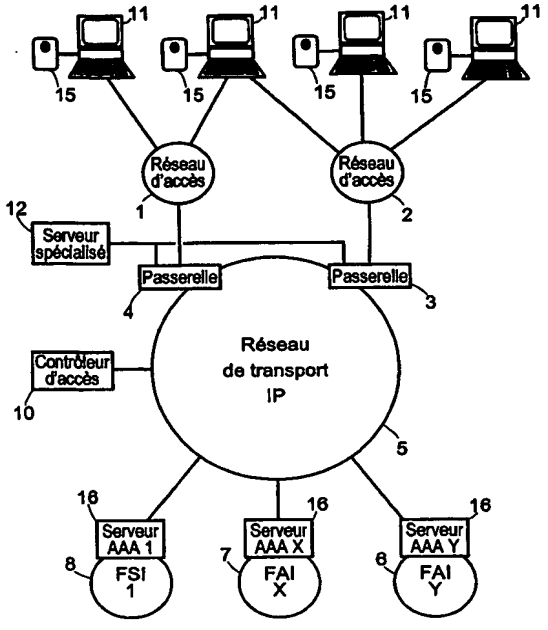
(74) Mandataires : **PICHAT, Thierry** etc.; Novograaf Technologies, 122, rue Edouard Vaillant, F-92593 Levallois Perret Cedex (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB,

[Suite sur la page suivante]

(54) Title: METHOD AND SYSTEM FOR DOUBLE SECURED AUTHENTICATION OF A USER DURING ACCESS TO A SERVICE BY MEANS OF A DATA TRANSMISSION NETWORK

(54) Titre : PROCEDE ET SYSTEME DE DOUBLE AUTHENTIFICATION SECURISEE D'UN UTILISATEUR LORS DE L'ACCES A UN SERVICE PAR L'INTERMEDIAIRE D'UN RESEAU DE TRANSMISSION DE DONNEES.



1, 2... ACCESS NETWORK
4, 3... GATEWAY
5... IP TRANSPORT NETWORK
6, 7... INTERNET ACCESS PROVIDERS X AND Y
8... INTERNET SERVICE PROVIDER 1
10... ACCESS CONTROLLER
12... SPECIAL SERVER
16... SERVERS AAA 1, AAA X AND AAA Y

(57) **Abstract:** The invention relates to a method for authentication of a user during access to services provided by a data transmission network (5) consisting in transmitting a random number to a user terminal (11), cryptographically calculating authentication data of a user with two actuators (6, 7, 8) of the network (5) with the aid of secret keys proposed by the user, introducing identification data and calculated authentication data into the access request and in transmitting said access request by the terminal (11) to an access controller (10) which transmits a respective authentication request containing the identification and authentication data of the user to each actuator, carrying out an identification procedure (28, 29) by each actuator on the basis of the user identification and authentication data containing in the authentication requests and emitting authentication reports containing authentication results to the terminal (11).

(57) **Abrégé :** Procédé d'authentification d'un utilisateur lors d'un accès à des services offerts par un réseau de transmission de données (5), dans lequel : un nombre aléatoire est transmis à un terminal (11) d'utilisateur ; des données d'authentification de l'utilisateur auprès de deux acteurs (6, 7, 8) du réseau (5) sont calculées par cryptographie à l'aide de clés secrètes propres à l'utilisateur, le terminal (11) insère dans une requête d'accès des données d'identification et les données d'authentification calculées, et transmet la requête à un contrôleur d'accès (10) qui transmet à chacun des deux acteurs une requête d'authentification respective contenant les données d'identification et d'authentification de l'utilisateur ; chacun des acteurs exécute une procédure d'authentification (28, 29), sur la base des données d'identification et d'authentification

[Suite sur la page suivante]

WO 2005/020538 A2

GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **États désignés** *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

de l'utilisateur, contenues dans les requêtes d'authentification, et émettent des comptes rendus d'authentification contenant les résultats des procédures d'authentification, à destination du terminal (11).